IT Unit 3

Topic 2

# Ch 3, Data Analytics: Drawing Conclusions, Part 2

**Data security**, 170-175

1. Why is data security important to an organisation?

* Loss of reputation
* Vital for the functioning of the business or organisation
* Loss of business
* Might find themselves in a court case surrounding the privacy act 1988

1. Distinguish between deliberate and accidental threats to data.

* Deliberate refers to programs and hackers that have intentionally tried to steal or damage data that they have no right to. While accidental refers to things such as natural disasters, technical failures and human error.

**Physical security**

1. List ways of physically security data.

* Keeping your laptop or tablet in a secure place when you’re not using it such as a locked cabinet.
* Not letting people that you don’t know that well use your devices
* Making sure family and friends cannot access important data if they need to use your device
* Keeping doors and windows locked to prevent theft of hardware
* If you use a desktop computer keep it switched off when you are not using it
* Consider using surge-protector power outlets for all of your devices to protect data.

**Software security**

1. Elaborate under each of the following software security strategies:
   1. Use strong passwords

* When selecting a password try to make it at least 8 characters long, include a combination of alphanumeric characters and use of both capital and lowercase characters.
  1. Use login passwords
* We should have a login password on all of our devices, to try and prevent the risk of losing it or having it stolen and having someone else switch it on and have immediate access to everything you have stored on it.
  1. Use biometric identification
* Can be used to control computers and resources when the user is physically present, it cannot be lost, stolen, guessed or discovered easily and is utterly unique.
  1. Always log out
* We log out because if we don’t we leave ourselves and our data vulnerable to anyone who walks past and sees the computer logged in.
  1. Encryption
     1. What is public key encryption
* It’s a system that encrypts the data and can only be opened using two keys, the public key and the private or secret key known only by the recipient of the message.
  + 1. What is PGP?

Pretty good privacy, it’s a software that uses public key encryption to protect their documents.

* 1. Firewall
* Used to prevent unauthorised access to your data and information, and deny network access to outsiders.
  1. Antivirus software
     1. What is malware?
* It’s a malicious software that has intent on either stealing or damaging your data, files and system.
  + 1. What is payload?
* The destructive potential of malware.
  1. Backup your files
* Because despite all of your best efforts, disasters may and still can happen. So data backups are the final defence against total data loss.